

- 17 -

WE CLAIM:

1. A method for allocating to a device a licence to use digital content, the method comprising the steps of:
- 5 receiving a first block of ciphertext from the device;
- decrypting the first block of ciphertext to obtain a second block of ciphertext;
- 10 determining whether the second block of ciphertext meets a criterion; and
- allocating the licence to the device if the second block of ciphertext meets the criterion.
- 15 2. The method as claimed in claim 1, wherein the step of allocating the licence comprises the steps of:
- encrypting the first block of ciphertext to obtain a third block of ciphertext;
- obtaining a usage right for the digital content;
- 20 and
- providing the device with the third block of ciphertext and an encrypted version of the usage right.
- 25 3. The method as claimed in claim 1 or 2, wherein the step of determining whether the second block of ciphertext meets the criterion comprises the step of determining whether the second block of ciphertext corresponds to a last block of ciphertext received in
- 30 relation to a request for the licence.
4. The method as claimed in claim 3, wherein the step of allocating the licence comprises the step of updating the last block of ciphertext such that it
- 35 corresponds to the first block of ciphertext.

- 18 -

5. The method as claimed in claim 3 or 4,
further comprising the steps of:

determining whether there exists a previous block
of ciphertext that was received in relation to another
5 request for a licence and which corresponds to the second
block of ciphertext; and

issuing the device with a notification that the
licence has expired if it is determined that the previous
block of ciphertext exists and was obtained prior to the
10 last block of ciphertext being obtained;

wherein the steps of determining whether there
exists a previous block, and issuing the device with the
notification are carried out upon determining that the
second block of ciphertext does not meet the criterion.

15

6. The method as claimed in any one of claims 1
to 5, wherein the licence is arranged to expire after a
predetermined period of time.

20

7. A method of requesting a licence to use
digital content, the method comprising the steps of:

obtaining a first block of ciphertext from a
system arranged to allocate the licence;

encrypting the first block of ciphertext to
25 obtain a second block of ciphertext; and

providing the second block of ciphertext to the
system when requesting the licence.

30

8. The method as claimed in claim 7, further
comprising the step of providing the second block of
ciphertext to another device for use thereby when
requesting the licence.

35

9. A system for allocating a device with a
licence to use digital content, the system comprising
processing means arranged to perform the steps of:

receiving a first block of ciphertext from the

- 19 -

device ;

decrypted the first block of ciphertext to
obtain a second block of ciphertext;

determining whether the second block of
5 ciphertext meets a criterion; and
allocating the licence to the device if the
second block of ciphertext meets the criterion.

10 10. The system as claimed in claim 9, wherein
the processing means is arranged to perform the following
steps when allocating the licence to the device:

encrypting the first block of ciphertext to
obtain a third block of ciphertext;
obtaining a usage right for the digital content;

15 and

providing the device with the third block of
ciphertext and an encrypted version of the usage right.

11. The system as claimed in claim 9 or 10,
20 wherein the processing means is arranged to perform the
following step when determining whether the second block of
ciphertext meets the criterion: determining whether the
second block of ciphertext corresponds to a last block of
ciphertext received in relation to a request for the
25 licence.

12. The system as claimed in claim 11, wherein
the processing means is arranged to perform the step of
updating the last block of ciphertext such that it
30 corresponds to the first block of ciphertext when
allocating the licence.

13. The system as claimed in claim 11 or 12,
wherein the processing means is arranged to perform the
35 following steps:
determining whether there exists a previous block
of ciphertext that was received in relation to another

- 20 -

request for a licence and which corresponds to the second block of ciphertext; and

issuing the device with a notification that the licence has expired if it is determined that the previous
5 block of ciphertext exists and was obtained prior to the last block of ciphertext being obtained;

wherein the steps of determining whether there exists a previous block, and issuing the device with the notification are carried out upon determining that the
10 second block of ciphertext does not meet the criterion.

14. The system as claimed in any one of claims 9 to 13, wherein the licence is arranged to expire after a predetermined period of time.

15

15. A device for requesting a licence to use digital content, the device comprising a processing means arranged to perform the following steps:

obtaining a first block of ciphertext from a
20 system arranged to allocate the licence;

encrypting the first block of ciphertext to obtain a second block of ciphertext; and

providing the second block of ciphertext to the system when requesting the licence.

25

16. The device as claimed in claim 15, wherein the processing means is arranged to perform the step of providing the second block of ciphertext to another device for use thereby when requesting the licence.

30

17. A computer program comprising at least one instruction for causing a computing device to carry out the method as claimed in any one of claims 1 to 8.

35

18. A computer readable medium comprising the computer program claimed in claim 17.